

10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044

5

This invention relates to random number generation in a digital system.

Background of the Invention

Certain communications buses can receive and transfer 16 bits of data per clock cycle. Pseudo-random numbers (PRNs) are conventionally generated as 8 bits per clock cycle by a linear feedback shift register (LFSR), which cannot meet the throughput requirements for a 16-bit cycle.

What is needed is a system that generates a 16-bit PRN per clock cycle, utilizing the reliable technology developed to provide 8-bit PRNs. Preferably, this approach should be flexible and allow use of a variety of characteristic equations with corresponding LFSR configurations.

Summary of the Invention

20

Brief Description of the Drawings

Figures 1A and 1B schematically illustrate conventional generation of an 8-bit PRN.

Figures 2 and 3 schematically illustrate generation of 16-bit PRNs according to two embodiments of the invention.

Description of Best Modes of the Invention

Figure 1 schematically illustrates a conventional system 11 for generating an 8-bit PRN within one clock cycle, using type D flipflops that are triggered on a rising clock signal edge. The particular LFSR configuration shown in Figure 1 corresponds to the characteristic polynomial

$$p_1(x;8) = 1 + x^2 + x^3 + x^4 + x^8, \quad (1)$$

where x is an unspecified element of a field and a "1" coefficient (always present) for the highest degree (x^8) indicates that this stage is connected to a stage in another level. The system 11 shown in Figure 1, corresponding to the characteristic polynomial $p(x;8)$ in Eq. (1), has 255 different non-zero value n-tuples ($v_0, v_1, v_2, v_3, v_4, v_5, v_6, v_7$) (with $n = 8$) and has a minimum cycle length of 255. The cycle generated by this LFSR system is irreducible in the sense that the polynomial $p_1(x;8)$ cannot be expressed as the product of two or more polynomials of degree less than 8. S.B. Wicker, in Error Control Systems for Digital Communication and Storage, Prentice Hall, Upper Saddle River, NJ, 1995, pp. 445-447, lists 16 degree-8 irreducible polynomials:

$$p(x;8) = 1 + x^4 + x^5 + x^6 + x^8;$$

$$p(x;8) = 1 + x^3 + x^5 + x^7 + x^8;$$

$$p(x;8) = 1 + x^3 + x^5 + x^6 + x^8;$$

$$p(x;8) = 1 + x^2 + x^5 + x^6 + x^8;$$

$$p(x;8) = 1 + x^2 + x^4 + x^5 + x^6 + x^7 + x^8;$$

$$p(x;8) = 1 + x^2 + x^3 + x^7 + x^8;$$

$$p(x;8) = 1 + x^2 + x^3 + x^6 + x^8;$$

$$p(x;8) = 1 + x^2 + x^3 + x^5 + x^8;$$

$$p(x;8) = 1 + x^2 + x^3 + x^4 + x^8;$$

$$p(x;8) = 1 + x^2 + x^6 + x^7 + x^8;$$

$$p(x;8) = 1 + x + x^5 + x^6 + x^8;$$

$$p(x;8) = 1 + x + x^3 + x^5 + x^8;$$

$$p(x;8) = 1 + x + x^2 + x^7 + x^8;$$

$$p(x;8) = 1 + x + x^2 + x^5 + x^6 + x^7 + x^8;$$

$$p(x;8) = 1 + x + x^2 + x^3 + x^6 + x^7 + x^8; \text{ and}$$

$$p(x;8) = 1 + x + x^2 + x^3 + x^4 + x^6 + x^8. \quad (2)$$

In Figure 1, a reset signal is received or a feedback digital signal S(in) is received on an input signal line 13 and distributed to a data signal input terminal of each of eight type D flipflops (FFs), numbered 17-i (i = 0, 1, ... , 7). A clock signal CLK(t) is received on a clock input signal line 15 and is distributed to a clock input terminal each of the eight FFs 17-i. A single bit first output signal S(t;i;out1) (i = 0, 1, 2) from the FF 17-i is received by one of three input terminals of an AND gate 21 that forms and issues a first intermediate output signal S(t;0/1/2;out1) = S(t;0;out1)·S(t;1;out1)·S(t;2;out1). A single bit output signal S(t;i;out) (i = 3, 4, 5, 6) from the FF 17-i is received by one of three input terminals of an AND gate 23 that forms and issues a second intermediate output signal S(t;3/4/5/6;out1) = S(t;3;out1)·S(t;4;out1)·S(t;5;out1)·S(t;6;out1). These first and second intermediate output signals are received by a two-terminal OR gate 25 that forms and issues a third intermediate output signal

$S(t;0/1/2/3/4/5/6;out1) = S(t;0/1/2;out1) \oplus S(t;3/4/5/6;out1)$. An output of the OR gate 25 is received by a first input terminal of an XOR gate 27.

A complementary single-bit output signal $S(t;j1;out2) = S(t;j2;out1)^*$ is issued by the FFs 17-j1 ($j1 = 1,2,3$) and is received by a first input terminal of an XOR gate 19-(j1+1).

A complementary single-bit second output signal $S(t;j2;out2) = S(t;j2;out1)^*$ ($j2 = 0, 4, 5, 6$) is issued by the FF 17-j2 and is received by a signal input terminal of the FF 17-(j2+1). A single bit complementary output signal $S(t;7;out2) = S(t;7;out1)^*$ is issued by the FF 17-7 and is received by a second input terminal of the XOR gate 27. The output signal of the XOR gate 27 is fed back to, and received by, a second input terminal of the XOR gates 19-2, 19-3 and 19-4 and by the signal input terminal of the FF 17-0. The output signals $S(t;j3;out2)$ ($j3 = 0, 1, 2, 3, 4, 5, 6, 7$), collectively referred to as $S(t;out)$, are received in serial order by an output signal line 29 as an eight-bit pseudo-random number (PRN) from the device 11. The configuration shown in Figure 1 provides an eight-bit PRN $S(t;out)$ with each clock cycle. Using any of Eqs. (2) for the characteristic polynomial, the system 11 generates an ordered sequence of 255 different, non-zero value n-tuples ($n = 8$).

Figure 2 schematically illustrates a system 111 for generating a 16-bit PRN $S(t;out)$ within one clock cycle according to the invention, using a first 8-bit LFSR 112A that is triggered on a rising clock signal edge and a second 8-bit LFSR 112B that is triggered on a falling clock signal edge during the same clock cycle. The particular LFSR configurations shown in Figure 2 correspond to the (same) irreducible characteristic polynomial, for example,

$$pA(x;8) = pB(x;8) = 1 + x^2 + x^3 + x^4 + x^8. \quad (3)$$

10 15

5

10 20 30 40 50 60 70 80 90 100

20

25

received at the input terminal of the FF 157-(i4+1) and by the output line 131. A Q* output signal from the FF 117-7 is received by a second input terminal of the XOR 127 and by the output line 131.

An output signal on an intermediate line 129 from the XOR gate 127 is fed to an input signal terminal of the FF 157-0 (analogous to feedback to the first FF 17-0 in Figure 1). This fed-back signal on the line 129 is also received and processed by a second input terminal of the XOR gates 159-i5 (i5 = 2, 3, 4); and the output signal of the XOR gate 159-i5 is received by a data input terminal of the FF 157-i5.

A Q output signal from the FF 157-i6 (i6 = 0, 4, 5, 6) is received by the FF 117-(i6+1) and by the output line 131. A Q output signal from the FF 157-i7 (i7 = 1, 2, 3) is received by the XOR gate 119-(i7+1) and by the output line 131. A Q* output signal from the FF 157-i8 (i8 = 0, 1, 2) is received by a three-input terminal AND gate 161. A Q* output signal from the FF 157-i9 (i9 = 3, 4, 5, 6) is received by a four-input terminal AND gate 163. The output signals from the AND gates 161 and 163 are received by two input terminals of an OR gate 165, whose output signal is received by a first input terminal of an XOR gate 167. The output line 131 and a second input terminal of the XOR gate 167 receive a Q output signal from the FF 157-7. An output signal from the XOR gate 167 is received on a signal line 169 by a control or clock signal terminal of the FF 117-0.

Eight bits of a 16-bit output signal S(t;out) are provided by one output signal (Q*) from each of the FFs 117-i (i = 0, 1, ... , 7), and these bits are issued on a rising clock signal (or on a falling clock signal). Another eight bits of the 16-bit output signal S(t;out) are provided by one output signal (Q) from each of the FFs 157-i (i = 0, 1, ... , 7), and these bits are issued on a falling clock signal (or on

a rising clock signal). Optionally, the output signals from the FFs 117-i and/or the output signals from the FFs 157-i ($i = 0, 1, \dots, 7$) are passed through delay modules with selected time delays to control any race problem that might otherwise occur. The entire 16 bits of the output signal $S(t;out)$ are thus issued within a single clock cycle, after computation within a preceding clock cycle. The eight bits (Q^*) issuing from the FFs 117-i and the eight bits (Q) issuing from the FF 157-i may be interleaved in an arbitrary manner or may be concatenated to provide a 16-bit PRN that does not repeat itself for any cycle of length at least 255 and no greater than 65,535.

The two n-tuples provided by the LFSR configurations 112A and 112B can be concatenated to provide the following concatenated sequences, among others:

$$C1 = (v0, v1, v2, v3, v4, v5, v6, v7, v8, v9, v10, v11, v12, v13, v14, v15), \quad (4)$$

$$C2 = (v8, v9, v10, v11, v12, v13, v14, v15, v0, v1, v2, v3, v4, v5, v6, v7). \quad (5)$$

The two n-tuples provided by the LFSR configurations 112A and 112B can be interleaved in any of $15!$ permutations, including the following sequences:

$$I1 = (v0, v8, v1, v9, v2, v10, v3, v11, v4, v12, v5, v13, v6, v14, v7, v15), \quad (6)$$

$$I2 = (v15, v1, v14, v2, v13, v3, v12, v4, v11, v5, v10, v6, v9, v7, v8, v0), \quad (7)$$

$$I3 = (v5, v8, v14, v2, v3, v11, v15, v1, v13, v0, v4, v12, v9, v6, v10, v7). \quad (8)$$

The first and second LFSR configurations, 112A and 112B, include eight rising edge (positively triggered) D-flipflops and eight falling edge (negatively triggered) D-flipflops. Alternatively, the rising edge and falling edge FF signals can be exchanged with each other.

At least three unusual features are relied upon in this invention. First, feedback from a rising edge LFSR configuration is received by a falling edge LFSR configuration, and conversely. Second, The FFs within each of the first

and second LFSR configurations operate without an input tap. Individually, the first and second LFSR configurations do not operate as standard LFSRs in Figure 2. Third, at least one of (and preferably both of) the two LFSR configurations, 112A and 112B, should correspond to an irreducible polynomial, but the system will work where only one of the two characteristic polynomials is irreducible. If each of the two characteristic polynomials is a different irreducible polynomial, the minimum cycle length becomes 65,535.

The three-input and four-input AND gates, 121 and 123, or 161 and 163, in Figure 2 can be replaced by two AND gates with m1 and 7-m1 input terminals, respectively, where m1 = 2, 3, 4 and 5.

Figure 3 schematically illustrates a system 211 for generating a 16-bit PRN S(t;out) within one clock cycle according to another embodiment of the invention, using a first 8-bit LFSR 212A that is triggered on a rising clock signal edge and a second 8-bit LFSR 212B that is triggered on a falling clock signal edge during the same clock cycle. The first and second LFSR configurations shown in Figure 32 correspond to the respective irreducible characteristic polynomials

$$pA(x;8) = 1 + x^2 + x^3 + x^5 + x^8, \quad (9A)$$

$$pB(x;8) = 1 + x^2 + x^3 + x^5 + x^8. \quad (9B)$$

Signals for the LFSRs 212A and 212B preferably transition during a rising clock signal edge and during a falling clock signal edge, respectively, or during a falling clock signal edge and during a rising clock signal edge, respectively. The particular irreducible characteristic polynomials, pA(x;8) and pB(x;8), set forth in Eqs. (9A) and (9B), implemented as shown in the LFSR configurations of Figure 3, are another example of a degree-eight characteristic polynomial. Optionally, the output signals from the FFs 217-i and/or the output signals from the FFs 257-i

($i = 0, 1, \dots, 7$) are passed through delay modules with selected time delays to control any race problem that might otherwise occur.

Each of the first LFSR configuration 212A and the second LFSR configuration 212B performs as discussed in connection with the analogous LFSRs, 112A and 112B, in Figure 2, but with a different characteristic polynomial, set forth in Eqs. (9A) and (9B).

10
T08260" 49599660